Refine Search

Search Results -

Terms	Documents
L12 and (rule or condition)	1

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L15

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Saturday, September 25, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L15	L12 and (rule or condition)	1	L15
L14	L12 and (hash$ and compar$)	1	L14
L13	L12 and (hash$ same compar$)	0	L13
L12	5715403.pn.	1	L12
L11	L6 and ((another or additon$ or new or extra) near2 cop$)	10	L11
L10	L6 and ((another or new or extra) near3 cop$).clm.	1	L10
L9	L8 and l7	0	L9
L8	L6 and ((another or new or extra) with cop$).clm.	1	L8
L7	L6 and (addition$ with cop$).clm.	1	L7
L6	L5 and l1	153	L6
L5	L4 or l3 or l2	2500	L5
L4	705/57,51,59.ccls.	645	L4
L3	380/28,30.ccls.	1265	L3

h e b b cg b e e ch

L2	713/176,170,181.ccls.	825	L2
L1	((addition$ or new or extra or another) with cop$) and (encrypt$ or decrypt$ or crypto$) and @ad<=20001113	1447	L1

END OF SEARCH HISTORY

Generate Collection Print

L11: Entry 10 of 10 File: USPT Feb 3, 1998

US-PAT-NO: 5715403
DOCUMENT-IDENTIFIER: US 5715403 A

TITLE: System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar

DATE-ISSUED: February 3, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Stefik; Mark J.	Woodside	CA		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Xerox Corporation	Stamford	CT			02

APPL-NO: 08/ 344041 [PALM]
DATE FILED: November 23, 1994

INT-CL: [06] G06 F 1/14, G06 F 13/372

US-CL-ISSUED: 395/244; 395/188.01, 395/800, 380/23
US-CL-CURRENT: 705/44; 705/54, 705/57, 709/229, 713/202

FIELD-OF-SEARCH: 395/800, 395/600, 395/700, 395/775, 395/650, 395/182.13, 395/608, 395/183.14, 395/201, 395/569, 395/825, 395/712, 395/187.01, 395/188.01, 395/244, 395/217, 380/4, 380/15, 380/18, 380/20, 380/25, 380/24, 380/23, 380/30, 364/DIG.1, 364/DIG.2, 364/41R, 340/825.33, 340/825.34, 348/3, 455/4.1, 455/5.1, 455/26.1

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	3790700	February 1974	Callais et al.	348/3
☐	4529870	July 1985	Chaum	235/380
☐	4658093	April 1987	Hellman	380/25
☐	4891838	January 1990	Faber	380/25
☐	4924378	May 1990	Hershey et al.	364/200

h e b b g e e e f c e h e ge

☐	4932054	June 1990	Chou et al.	380/4
☐	4937863	June 1990	Robert et al.	380/4
☐	4953209	August 1990	Ryder, Sr. et al.	380/23
☐	4961142	October 1990	Elliott et al.	364/408
☐	4977594	December 1990	Shear	380/4
☐	5010571	April 1991	Katznelson	380/4
☐	5014234	May 1991	Edwards, Jr.	364/900
☐	5023907	June 1991	Johnson et al.	380/4
☐	5047928	September 1991	Wiedemer	364/406
☐	5050213	September 1991	Shear	380/25
☐	5058164	October 1991	Elmer et al.	380/50
☐	5103476	April 1992	Waite et al.	380/4
☐	5113519	May 1992	Johnson et al.	395/600
☐	5138712	August 1992	Corbin	395/700
☐	5146499	September 1992	Geffrotin	380/23
☐	5159182	October 1992	Eisele	235/492
☐	5191193	March 1993	Le Roux	235/379
☐	5204897	April 1993	Wyman	380/4
☐	5247575	September 1993	Sprague et al.	380/9
☐	5255106	October 1993	Castro	380/18
☐	5260999	November 1993	Wyman	380/4
☐	5291596	March 1994	Mita	395/608
☐	5339091	August 1994	Yamazaki et al.	345/104

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0332707	September 1989	EP	
2236604	April 1991	GB	
WO9220022	November 1992	WO	
9301550	January 1993	WO	

OTHER PUBLICATIONS

Press Release From Electronic Publishing Resources, Inc. (EPR) entitled "National Semiconductor and EPR Partner for Information Metering/Data Security Cards", dated Mar. 4, 1994.
Weber, R., "Digital Rights Management Technology", Oct. 1995.
European Search Report for Corresponding European Application 95308417.5.
U. Flasche et al., Decentralized Processing of Documents, Comput. & Graphics, vol. 10, No. 2, 1986, pp. 119-131.
R. Mori et al., Superdistribution: The Concept and the Architecture, The Transactions of the IEICE, vol. E 73, No. 7, 1990, Tokyo, JP, pp. 1133-1146.

h e b b g e e e f c e h e ge

Weber, R., "Metering Technologies For Digital Intellectual Property," A Report to the International Federation of Reproduction Rights Organizations, Oct. 1994, pp. 1-29.
Clark, P.C. and Hoffman, L.J., "Bits: A Smartcard Protected Operating System," Communications of the ACM, Nov. 1994, vol. 37, No. 11, pp. 66-70, and 94.
Ross, P.E., "Data guard", Forbes, Jun. 6, 1994, p. 101.
Saigh, W.K., "Knowledge is Sacred," Video Pocket/Page Reader Systems, Ltd., 1992.
Kahn, R.E., "Deposit, Registration And Recordation In An Electronic Copyright Management System," Corporation for National Research Initiatives, Virginia, Aug. 1992, pp. 1-19.
Hilts, P., Mutter, J., and Taylor, S., "Books While U Wait," Publishers Weekly, Jan. 3, 1994, pp. 48-50.
Strattner, A., `"Cash register on a chip" may revolutionize software pricing and distribution; Wave Systems Corp.,` Computer Shopper. Copyright, Apr. 1994, vol. 14; No. 4; p. 62; ISSN 0886-0556.
O'Conner, M.A., "New distribution option for electronic publishers; iOpener data encryption and metering system for CD-ROM use; Column," CD-ROM Professional, Copyright, Mar. 1994, vol. 7; No. 2; p. 134; ISSN: 1049-0833.
Willett, S., `"Metered PCs: Is your system watching you?"; Wave Systems beta tests new technology,` InfoWorld, Copyright, May 2, 1994, p. 84.
Linn, R.J., "Copyright and Information Services in the Context of the National Research and Education Network.sup.1," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 9-20.
erritt, Jr., H.H., "Permissions Headers and Contract Law," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 27-48.
Upthegrove, L., and Roberts, R., "Intellectual Property Header Descriptors: A Dynamic Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 63-66.
Sirbu, M.A., "Internet Billing Service Design and Prototype Implementation," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 67-80.
Simmel, S.S., and Godard, I., "Metering and Licensing of Resources: Kala's General Purpose Approach," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 81-110.
Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 111-120.
Tygar, J.D., and Bennet, Y., "Dyad: A System for Using Physically Secure Coprocessors," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 121-152.
Griswold, G.N., "A Method for Protecting Copyright on Networks," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 169-178.
Nelson, T.H., "A Publishing and Royalty Model for Networked Documents," IMA Intellectual Property Project Proceedings, Jan. 1994, vol. 1, Issue 1, pp. 257-259.

ART-UNIT: 232

PRIMARY-EXAMINER: Pan; Daniel H.

ATTY-AGENT-FIRM: Domingo; Richard B.

ABSTRACT:

A system for controlling use and distribution of digital works. The present invention allows the owner of a digital work to attach usage rights to their work. The usage rights define how the individual digital work may be used and distributed. Instances of usage rights are defined using a flexible and extensible usage rights grammar. Conceptually, a right in the usage rights grammar is a label associated with a predetermined behavior and conditions to exercising the right.

h e b b g e e e f c e h e ge

The behavior of a usage right is embodied in a predetermined set of usage transactions steps. The usage transaction steps further check all conditions which must be satisfied before the right may be exercised. These usage transaction steps define a protocol for requesting the exercise of a right and the carrying out of a right.

28 Claims, 20 Drawing figures

Previous Doc Next Doc Go to Doc#

h e b b g e e e f c e h e ge

L11: Entry 10 of 10 File: USPT Feb 3, 1998

DOCUMENT-IDENTIFIER: US 5715403 A
TITLE: System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar

Application Filing Date (1):
19941123

Brief Summary Text (20):
U.S. Pat. No. 5,247,575, Sprague et al., entitled "Information Distribution System", describes an information distribution system which provides and charges only for user selected information. A plurality of encrypted information packages (IPs) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. Some of the IPs may be of no interest to the user. The IPs of interest are selected by the user and are decrypted and stored locally. The IPs may be printed, displayed or even copied to other storage medias. The charges for the selected IP's are accumulated within a user apparatus and periodically reported by telephone to a central accounting facility. The central accounting facility also issues keys to decrypt the IPs. The keys are changed periodically. If the central accounting facility has not issued a new key for a particular user station, the station is unable to retrieve information from the system when the key is changed.

Brief Summary Text (21):
A system available from Wave Systems Corp. of Princeton, N.Y., provides for metering of software usage on a personal computer. The system is installed onto a computer and collects information on what software is in use, encrypts it and then transmits the information to a transaction center. From the transaction center, a bill is generated and sent to the user. The transaction center also maintains customer accounts so that licensing fees may be forwarded directly to the software providers. Software operating under this system must be modified so that usage can be accounted.

Detailed Description Text (55):
FIG. 3 illustrates the repository 201 coupled to a credit server 301. The credit server 301 is a device which accumulates billing information for the repository 201. The credit server 301 communicates with repository 201 via billing transactions 302 to record billing transactions. Billing transactions are reported to a billing clearinghouse 303 by the credit server 301 on a periodic basis. The credit server 301 communicates to the billing clearinghouse 303 via clearinghouse transactions 304. The clearinghouse transactions 304 enable a secure and encrypted transmission of information to the billing clearinghouse 303.

Detailed Description Text (58):
FIG. 4a illustrates a printer as an example of a rendering system. Referring to FIG. 4, printer system 401 has contained therein a printer repository 402 and a print device 403. It should be noted that the dashed line defining printer system 401 defines a secure system boundary. Communications within the boundary is assumed to be secure. Depending on the security level, the boundary also represents a

barrier intended to provide physical integrity. The printer repository 402 is an instantiation of the rendering repository 205 of FIG. 2. The printer repository 402 will in some instances contain an ephemeral copy of a digital work which remains until it is printed out by the print engine 403. In other instances, the printer repository 402 may contain digital works such as fonts, which will remain and can be billed based on use. This design assures that all communication lines between printers and printing devices are encrypted, unless they are within a physically secure boundary. This design feature eliminates a potential "fault" point through which the digital work could be improperly obtained. The printer device 403 represents the printer components used to create the printed output.

Detailed Description Text (64):
FIG. 5 illustrates the layout of a contents file. Referring to FIG. 5, a digital work 509 is comprised of story A 510, advertisement 511, story B 512 and story C 513. It is assumed that the digital work is stored starting at a relative address of 0. Each of the parts of the digital work are stored linearly so that story A 510 is stored at approximately addresses 0-30,000, advertisement 511 at addresses 30,001-40,000, story B 512 at addresses 40,001-60,000 and story C 513 at addresses 60,001-85K. The detail of story A 510 is illustrated in FIG. 6. Referring to FIG. 6, the story A 510 is further broken down to show text 614 stored at address 0-1500, soldier photo 615 at addresses 1501-10,000, graphics 616 stored at addresses 10,001-25,000 and sidebar 617 stored address 25,001-30,000. Note that the data in the contents file may be compressed (for saving storage) or encrypted (for security).

Detailed Description Text (86):
Communications integrity refers to the integrity of the communications channels between repositories. Roughly speaking, communications integrity means that repositories cannot be easily fooled by "telling them lies." Integrity in this case refers to the property that repositories will only communicate with other devices that are able to present proof that they are certified repositories, and furthermore, that the repositories monitor the communications to detect "impostors" and malicious or accidental interference. Thus the security measures involving encryption, exchange of digital certificates, and nonces described below are all security measures aimed at reliable communication in a world known to contain active adversaries.

Detailed Description Text (90):
As a prerequisite to operation, a repository will require possession of an identification certificate. Identification certificates are encrypted to prevent forgery and are issued by a Master repository. A master repository plays the role of an authorization agent to enable repositories to receive digital works. Identification certificates must be updated on a periodic basis. Identification certificates are described in greater detail below with respect to the registration transaction.

Detailed Description Text (92):
The hardware embodiment of a repository will be enclosed in a secure housing which if compromised, may cause the repository to be disabled. The basic components of the hardware embodiment of a repository are described with reference to FIG. 12. Referring to FIG. 12, a repository is comprised of a processing means 1200, storage system 1207, clock 1205 and external interface 1206. The processing means 1200 is comprised of a processor element 1201 and processor memory 1202. The processing means 1201 provides controller, repository transaction and usage rights transaction functions for the repository. Various functions in the operation of the repository such as decryption and/or decompression of digital works and transaction messages are also performed by the processing means 1200. The processor element 1201 may be a microprocessor or other suitable computing component. The processor memory 1202 would typically be further comprised of Read Only Memories (ROM) and Random Access Memories (RAM). Such memories would contain the software instructions utilized by

the processor element 1201 in performing the functions of the repository.

Detailed Description Text (98):
The repository specific functionality 1304 comprises functionality that is unique to a repository. For example, the master repository has special functionality for issuing digital certificates and maintaining encryption keys. The repository specific functionality 1304 would include the user interface implementation for the repository.

Detailed Description Text (110):
A credit server is a computational system that reliably authorizes and records these transactions so that fees are billed and paid. The credit server reports fees to a billing clearinghouse. The billing clearinghouse manages the financial transactions as they occur. As a result, bills may be generated and accounts reconciled. Preferably, the credit server would store the fee transactions and periodically communicate via a network with billing clearinghouse for reconciliation. In such an embodiment, communications with the billing clearinghouse would be encrypted for integrity and security reasons. In another embodiment, the credit server acts as a "debit card" where transactions occur in "real-time" against a user account.

Detailed Description Text (221):
Transactions require that there be some communication between repositories. Communication between repositories occurs in units termed as messages. Because the communication line is assumed to be unsecure, all communications with repositories that are above the lowest security class are encrypted utilizing a public key encryption technique. Public key encryption is a well known technique in the encryption arts. The term key refers to a numeric code that is used with encryption and decryption algorithms. Keys come in pairs, where "writing keys" are used to encrypt data and "checking keys" are used to decrypt data. Both writing and checking keys may be public or private. Public keys are those that are distributed to others. Private keys are maintained in confidence.

Detailed Description Text (222):
Key management and security is instrumental in the success of a public key encryption system. In the currently preferred embodiment, one or more master repositories maintain the keys and create the identification certificates used by the repositories.

Detailed Description Text (223):
When a sending repository transmits a message to a receiving repository, the sending repository encrypts all of its data using the public writing key of the receiving repository. The sending repository includes its name, the name of the receiving repository, a session identifier such as a nonce (described below), and a message counter in each message.

Detailed Description Text (224):
In this way, the communication can only be read (to a high probability) by the receiving repository, which holds the private checking key for decryption. The auxiliary data is used to guard against various replay attacks to security. If messages ever arrive with the wrong counter or an old nonce, the repositories can assume that someone is interfering with communication and the transaction terminated.

Detailed Description Text (225):
The respective public keys for the repositories to be used for encryption are obtained in the registration transaction described below.

Detailed Description Text (228):
The registration transaction between two repositories is described with respect to

FIGS. 16 and 17. The steps described are from the perspective of a "repository-1" registering its identity with a "repository-2". The registration must be symmetrical so the same set of steps will be repeated for repository-2 registering its identity with repository-1. Referring to FIG. 16, repository-1 first generates an encrypted registration identifier, step 1601 and then generates a registration message, step 1602. A registration message is comprised of an identifier of a master repository, the identification certificate for the repository-1 and an encrypted random registration identifier. The identification certificate is encrypted by the master repository in its private key and attests to the fact that the repository (here repository-1) is a bona fide repository. The identification certificate also contains a public key for the repository, the repository security level and a timestamp (indicating a time after which the certificate is no longer valid.) The registration identifier is a number generated by the repository for this registration. The registration identifier is unique to the session and is encrypted in repository-1's private key. The registration identifier is used to improve security of authentication by detecting certain kinds of communications based attacks. Repository-1 then transmits the registration message to repository-2, step 1603.

Detailed Description Text (229):
Upon receiving the registration message, repository-2 determines if it has the needed public key for the master repository, step 1604. If repository-2 does not have the needed public key to decrypt the identification certificate, the registration transaction terminates in an error, step 1618.

Detailed Description Text (230):
Assuming that repository-2 has the proper public key the identification certificate is decrypted, step 1605. Repository-2 saves the encrypted registration identifier, step 1606, and extracts the repository identifier, step 1607. The extracted repository identifier is checked against a "hotlist" of compromised document repositories, step 1608. In the currently preferred embodiment, each repository will contain "hotlists" of compromised repositories. If the repository is on the "hotlist", the registration transaction terminates in an error per step 1618. Repositories can be removed from the hotlist when their certificates expire, so that the list does not need to grow without bound. Also, by keeping a short list of hotlist certificates that it has previously received, a repository can avoid the work of actually going through the list. These lists would be encrypted by a master repository. A minor variation on the approach to improve efficiency would have the repositories first exchange lists of names of hotlist certificates, ultimately exchanging only those lists that they had not previously received. The "hotlists" are maintained and distributed by Master repositories.

Detailed Description Text (232):
Assuming that the repository is not on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that

the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.

Detailed Description Text (233):
At this point, assuming that the transaction has not terminated, the repositories exchange messages containing session keys to be used in all communications during the session and synchronize their clocks. FIG. 17 illustrates the session information exchange and clock synchronization steps (again from the perspective of repository-1.) Referring to FIG. 17, repository-1 creates a session key pair, step 1701. A first key is kept private and is used by repository-1 to encrypt messages. The second key is a public key used by repository-2 to decrypt messages. The second key is encrypted using the public key of repository-2, step 1702 and is sent to repository-2, step 1703. Upon receipt, repository-2 decrypts the second key, step 1704. The second key is used to decrypt messages in subsequent communications. When each repository has completed this step, they are both convinced that the other repository is bona fide and that they are communicating with the original. Each repository has given the other a key to be used in decrypting further communications during the session. Since that key is itself transmitted in the public key of the receiving repository only it will be able to decrypt the key which is used to decrypt subsequent messages.

Detailed Description Text (236):
A second session initiation transaction is a Login transaction. The Login transaction is used to check the authenticity of a user requesting a transaction. A Login transaction is particularly prudent for the authorization of financial transactions that will be charged to a credit server. The Login transaction involves an interaction between the user at a user interface and the credit server associated with a repository. The information exchanged here is a login string supplied by the repository/credit server to identify itself to the user, and a Personal Identification Number (PIN) provided by the user to identify himself to the credit server. In the event that the user is accessing a credit server on a repository different from the one on which the user interface resides, exchange of the information would be encrypted using the public and private keys of the respective repositories.

Detailed Description Text (276):
There are variations known in the art which can be used to achieve the same effect. For example, the server could use an additional level of encryption when transmitting a work to a client. Only after the client sends a message acknowledging receipt does it send the key. The client then agrees to pay for the digital work. The point of this variation is that it provides a clear audit trail that the client received the work. For trusted systems, however, this variation adds a level of encryption for no real gain in accountability.

Detailed Description Text (333):
A Backup transaction is a request to make a backup copy of a digital work, as a protection against media failure. In the context of repositories, secure backup copies differ from other copies in three ways: (1) they are made under the control of a Backup transaction rather than a Copy transaction, (2) they do not count as regular copies, and (3) they are not usable as regular copies. Generally, backup copies are encrypted.

Detailed Description Text (335):
The output of a Backup operation is both an encrypted data file that contains the contents and description of a work, and a restoration file with an encryption key

for restoring the encrypted contents. In many cases, the encrypted data file would have rights for "printing" it to a disk outside of the protection system, relying just on its encryption for security. Such files could be stored anywhere that was physically safe and convenient. The restoration file would be held in the repository. This file is necessary for the restoration of a backup copy. It may have rights for transfer between repositories.

Detailed Description Text (339):
The requester records the work contents, data, and usage rights. It then creates a one-time key and encrypts the contents file. It saves the key information in a restoration file.

Detailed Description Text (341):
In some cases, it is convenient to be able to archive the large, encrypted contents file to secure offline storage, such as a magneto-optical storage system or magnetic tape. This creation of a non-repository archive file is as secure as the encryption process. Such non-repository archive storage is considered a form of "printing" and is controlled by a print right with a specified "archive-printer." An archive-printer device is programmed to save the encrypted contents file (but not the description file) offline in such a way that it can be retrieved.

Detailed Description Text (343):
A Restore transaction is a request to convert an encrypted backup copy of a digital work into a usable copy. A restore operation is intended to be used to compensate for catastrophic media failure. Like all usage rights, restoration rights can include fees and access tests including authorization checks.

Detailed Description Text (347):
The server retrieves the key from the restoration file. It decrypts the work contents, data, and usage rights.

Detailed Description Text (374):
The requester sends the server a message to initiate an Extract transaction. This message indicates the part of the work to be extracted, the version of the extract right to be used in the transaction, the destination address information for placing the part as a new work, the file data for the work, and the number of copies involved.

Detailed Description Text (404):
The authorization server then "plays" the authorization. This involves decrypting it using either the public key of the master repository that issued the certificate or the session key from the repository that transmitted it. The authorization server then performs various tests. These tests vary according to the authorization server. They include such steps as checking issue and validity dates of the authorization and checking any hot-lists of known invalid authorizations. The authorization server may require carrying out any other transactions on the repository as well, such as checking directories, getting some person to supply a password, or playing some other digital work. It may also invoke some special process for checking information about locations or recent events. The "script" for such steps is contained within the authorization server.

Detailed Description Text (411):
The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step certifies the software.)

Detailed Description Text (412):
The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match

the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

Detailed Description Text (422):
The requester decrypts the digital certificate using the public key of the master repository, recording the identity of the supplier and creator, a key for decrypting the software, the compatibility information, and a tamper-checking code. (This step authenticates the certification of the software, including the script for uninstalling it.)

Detailed Description Text (423):
The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

Detailed Description Text (447):
A customer buys and uses the work. He cannot make new copies because he lacks a distribution license.

Detailed Description Text (449):
This is a variation on the previous scenarios. A distributor can sell to anyone and anyone can sell additional copies, resulting in fees being paid back to the creator. However, only licensed distributors can add fees to be paid to themselves.

45:4-9

Detailed Description Text (488):
The consumer goes to distributors and arranges to copy the work. The transaction offers the ticket. The distributor's repository punches the ticket and copies the new version to the consumers repository.

Detailed Description Text (496):
This scenario is like the common practice of people making cassette tapes to play in their car. If a publisher permits the making of cassette tapes, there is nothing to prevent a consumer from further copying the tapes. However, since the tapes are "analog copies," there is a noticeable quality loss with subsequent generations. The new contribution of the present invention is the use of tickets in the access controls for the making of the analog copies.

Detailed Description Text (512):
The information service bundles its database as files in a repository. The information services company assigns different fees for different rights on the information files. For example, there could be a fee for copying a search database or a source file and a different fee for printing. These fees would be in addition to fees assigned by the original creator for the services. The fees for using information would be different for using them on the information service company's computers or the client's computers. This billing distinction would be controlled by having different versions of the rights, where the version for use on the service company's computer requires a digital certificate held locally. Fees for copying or printing files would be handled in the usual way, by assigning fees to exercising those rights. The distinction between searching and viewing information would be made by having different "players" for the different functions. This distinction would be maintained on the client's computers as well as the service computers. Articles could be extracted for reuse under the control of Extract and Embed rights. Thus, if a client extracts part of an article or photograph, and then sells copies of a new digital work incorporating it, fees could automatically be collected both by the information service and earlier creators and distributors of the digital work. In this way, the information retrieval service could both offer a

wider selection of services and billing that more accurately reflects the client's use of the information.

Detailed Description Text (543):
A signed digital message that attests to the identity of the possessor. Typically, digital certificates are encrypted in the private key of a well-known master repository.

Detailed Description Text (546):
PUBLIC KEY ENCRYPTION:

Detailed Description Text (547):
An encryption technique used for secure transmission of messages on a communication channel. Key pairs are used for the encryption and decryption of messages. Typically one key is referred to as the public key and the other is the private key. The keys are inverses of each other from the perspective of encryption. Restated, a digital work that is encrypted by one key in the pair can be decrypted only by the other.

Detailed Description Paragraph Table (2):
TABLE 2 _____ REPOSITORY SECURITY LEVELS Level Description of Security _____ 0 Open system. Document transmission is unencrypted. No digital certificate is required for identification. The security of the system depends mostly on user honesty, since only modest knowledge may be needed to circumvent the security measures. The repository has no provisions for preventing unauthorized programs from running and accessing or copying files. The system does not prevent the use ofremovable storage and does not encrypt stored files. 1 Minimal security. Like the previous class except that stored files are minimally encrypted, including ones on removable storage. 2 Basic security. Like the previous class except that special tools and knowledge are required to compromise the programming, the contents of the repository, or the state of the clock. All digital communications are encrypted. A digital certificate is provided as identification. Medium level encryption is used. Repository identification number is unforgeable. 3 General security. Like the previous class plus the requirement of special tools are needed to compromise the physical integrity of the repository and that modest encryption is used on aIl transmissions. Password protection is required to use the local user interface. The digital clock system cannot be reset without authorization. No works would be stored on removable storage. When executing works as programs, it runs them in their own address space and does not give them direct access to any file storage or other memory containing system code or works. They can access works only through the transmission transaction protocol. 4 Like the previous class except that high level encryption is used on all communications. Sensors are used to record attempts at physical and electronic tampering. After such tampering, the repository will not perform other transactions until it has reported such tampering to a designated server. 5 Like the previous class except that if the physical or digital attempts at tampering exceed some preset thresholds that threaten the physical integrity of the repository or the integrity of digital and cryptographic barriers, then the repository will save only document description records of history but will erase or destroy any digital identifiers that could be misused if released to an unscrupulous party. It also modifies any certificates of authenticity to indicate that the physical system has been compromised. It also erases the contents ofdesignated documents. 6 Like the previous class except that the repository wiIl attempt wireless communication to report tampering and will employ noisy alarms. 10 This would correspond to a very high level of security. This server would maintain constant communications to remote security systems reporting transactions, sensor readings, and attempts to circumvent security.

Current US Cross Reference Classification (2):

h e b b g e e e f c e h e ge

705/57

Other Reference Publication (13):
O'Conner, M.A., "New distribution option for electronic publishers; iOpener data encryption and metering system for CD-ROM use; Column," CD-ROM Professional, Copyright, Mar. 1994, vol. 7; No. 2; p. 134; ISSN: 1049-0833.

Previous Doc Next Doc Go to Doc#

L14: Entry 1 of 1 File: USPT Feb 3, 1998

DOCUMENT-IDENTIFIER: US 5715403 A
TITLE: System for controlling the distribution and use of digital works having attached usage rights where the usage rights are defined by a usage rights grammar

Detailed Description Text (232):
Assuming that the repository is not on the hotlist, the repository identification needs to be verified. In other words, repository-2 needs to validate that the repository on the other end is really repository-1. This is termed performance testing and is performed in order to avoid invalid access to the repository via a counterfeit repository replaying a recording of a prior session initiation between repository-1 and repository-2. Performance testing is initiated by repository-2 generating a performance message, step 1609. The performance message consists of a nonce, the names of the respective repositories, the time and the registration identifier received from repository-1. A nonce is a generated message based on some random and variable information (e.g. the time or the temperature.) The nonce is used to check whether repository-1 can actually exhibit correct encrypting of a message using the private keys it claims to have, on a message that it has never seen before. The performance message is encrypted using the public key specified in the registration message of repository-1. The performance message is transmitted to repository-1, step 1610, where it is decrypted by repository-1 using its private key, step 1611. Repository-1 then checks to make sure that the names of the two repositories are correct, step 1612, that the time is accurate, step 1613 and that the registration identifier corresponds to the one it sent, step 1614. If any of these tests fails, the transaction is terminated per step 1616. Assuming that the tests are passed, repository-1 transmits the nonce to repository-2 in the clear, step 1615. Repository-2 then compares the received nonce to the original nonce, step 1617. If they are not identical, the registration transaction terminates in an error per step 1618. If they are the same, the registration transaction has successfully completed.

Detailed Description Text (234):
After the session information is exchanged, the repositories must synchronize their clocks. Clock synchronization is used by the repositories to establish an agreed upon time base for the financial records of their mutual transactions. Referring back to FIG. 17, repository-2 initiates clock synchronization by generating a time stamp exchange message, step 1705, and transmits it to repository-1, step 1706. Upon receipt, repository-1 generates its own time stamp message, step 1707 and transmits it back to repository-2, step 1708. Repository-2 notes the current time, step 1709 and stores the time received from repository-1, step 1710. The current time is compared to the time received from repository-1, step 1711. The difference is then checked to see if it exceeds a predetermined tolerance (e.g. one minute), step 1712. If it does, repository-2 terminates the transaction as this may indicate tampering with the repository, step 1713. If not repository-2 computes an adjusted time delta, step 1714. The adjusted time delta is the difference between the clock time of repository-2 and the average of the times from repository-1 and repository-2.

Detailed Description Text (412):

h e b b g e e e f c e h e ge

The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

Detailed Description Text (423):
The requester decrypts the software using the key from the certificate and computes a check code on it using a 1-way hash function. If the check-code does not match the tamper-checking code from the certificate, the installation transaction ends with an error. (This step assures that the contents of the software, including the various scripts, have not been tampered with.)

Previous Doc Next Doc Go to Doc#

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#
End of Result Set

Generate Collection Print

L7: Entry 1 of 1 File: USPT Jul 16, 2002

US-PAT-NO: 6421779
DOCUMENT-IDENTIFIER: US 6421779 B1
** See image for Certificate of Correction **

TITLE: Electronic data storage apparatus, system and method

DATE-ISSUED: July 16, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Kuroda; Yasutsugu	Kawasaki			JP
Kamada; Jun	Kawasaki			JP
Ono; Etsuo	Kawasaki			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Fujitsu Limited	Kawasaki			JP	03

APPL-NO: 09/ 123559 [PALM]
DATE FILED: July 29, 1998

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-313878	November 14, 1997

INT-CL: [07] H04 L 9/00

US-CL-ISSUED: 713/169; 713/170, 713/176, 713/180
US-CL-CURRENT: 713/169; 713/170, 713/176, 713/180

FIELD-OF-SEARCH: 705/57, 713/180, 713/181, 713/182, 713/165, 713/193, 713/194

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4458109	July 1984	Mueller-Schloer	380/30
☐	5606610	February 1997	Johansson	713/193

h e b b g e e e f c e h e ge

☐	5629982	May 1997	Micali	380/30
☐	5765152	June 1998	Erickson	707/9
☐	5958051	September 1999	Renaud et al.	
☐	5983295	November 1999.	Cotugno	710/74
☐	6021491	February 2000	Renaud	

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0 157 258	October 1985	EP	
0 354 774	February 1990	EP	
0 670 543	September 1995	EP	
0 718999	June 1996	EP	
2 205 667	December 1988	GB	
2 234 143	January 1991	GB	
2 242 104	September 1991	GB	
2 267 631	December 1993	GB	
10-326078	December 1998	JP	

ART-UNIT: 2132

PRIMARY-EXAMINER: Peeso; Thomas R.

ATTY-AGENT-FIRM: Staas & Halsey LLP

ABSTRACT:

An electronic data storage apparatus includes a data storage unit for storing electronic data; an authentication information generation unit for generating authentication information used in detecting an amendment made to the stored electronic data; and an authentication information data output unit for outputting the electronic data after adding to the electronic data the authentication information generated for the electronic data. When an authorization unit authorizes the electronic data storage apparatus after it is determined that the specification of the electronic data satisfies a predetermined condition, or when mutual authentication is performed between electronic data storage apparatuses, the electronic data storage apparatus stores the data. Thus, the electronic data can be protected from being illegally amended or deleted, and can be safely stored in a format in which sufficient legal evidence can be maintained on the electronic data.

54 Claims, 41 Drawing figures

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 4 of 4 returned.

1. Document ID: US 6199053 B1

L24: Entry 1 of 4 File: USPT Mar 6, 2001

US-PAT-NO: 6199053
DOCUMENT-IDENTIFIER: US 6199053 B1

TITLE: Digital signature purpose encoding

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

2. Document ID: US 6131162 A

L24: Entry 2 of 4 File: USPT Oct 10, 2000

US-PAT-NO: 6131162
DOCUMENT-IDENTIFIER: US 6131162 A

TITLE: Digital data authentication method

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

3. Document ID: US 6023509 A

L24: Entry 3 of 4 File: USPT Feb 8, 2000

US-PAT-NO: 6023509
DOCUMENT-IDENTIFIER: US 6023509 A

TITLE: Digital signature purpose encoding

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KWIC | Draw De

4. Document ID: US 5812669 A

L24: Entry 4 of 4 File: USPT Sep 22, 1998

US-PAT-NO: 5812669
DOCUMENT-IDENTIFIER: US 5812669 A

TITLE: Method and system for providing secure EDI over an open network

h e b b g e e e f e f ef b e

Full | Title | Citation | Front | Review | Classification | Date | Reference | | | Claims | KMC | Draw De

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L23 and (first adj hash$) and (second adj hash$)	4

Display Format: TI Change Format

Previous Page Next Page Go to Doc#

L24: Entry 1 of 4 File: USPT Mar 6, 2001

US-PAT-NO: 6199053
DOCUMENT-IDENTIFIER: US 6199053 B1

TITLE: Digital signature purpose encoding

DATE-ISSUED: March 6, 2001

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herbert; Howard C.	Phoenix	AZ		
Davis; Derek L.	Phoenix	AZ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Intel Corporation	Santa Clara	CA			02

APPL-NO: 09/ 287782 [PALM]
DATE FILED: April 8, 1999

PARENT-CASE:
This application is a continuation of Ser. No. 08/720,444 filed Sep. 30, 1996, U.S. Pat. No. 6,023,509.

INT-CL: [07] H04 L 9/00, H04 L 9/30

US-CL-ISSUED: 705/76; 380/29, 380/30, 713/175, 713/180
US-CL-CURRENT: 705/76; 380/29, 380/30, 713/175, 713/180

FIELD-OF-SEARCH: 705/50, 705/51, 705/64, 705/80, 705/26, 705/76, 380/29, 380/30, 380/42, 380/43, 380/287, 713/156, 713/157, 713/168, 713/173, 713/176, 713/177, 713/180, 713/182, 713/189, 713/200, 713/201

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5005200	April 1991	Fischer	713/176
☐	5208858	May 1993	Vollert et al.	380/43
☐	5479509	December 1995	Ugon	380/30
☐	6023509	February 2000	Herbert et al.	380/25

h e b b g e e e f c e f e ge

ART-UNIT: 362

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Blakely, Sokoloff, Taylor & Zafman LLP

ABSTRACT:

A method and apparatus for encoding a purpose into a digital signature, where purpose and digital signature bound into an extended digital signature. The extended digital signature capability binds a purpose description identifying the purpose for the digital signature so that when affixed to a digital signature, the digital signature cannot be employed for improper purposes. A hash function is used to generate a hash value from the purpose description. The hash value is used in a digital signature function to bind the purpose to a digital signature. The extended digital signature can be verified for validity by comparing it to a hash value. In an electronic transaction, the extended digital signature can allow a purpose to be bound with the digital signature so that improper or unauthorized transactions are detected and disallowed.

50 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

h e b b g e e e f c e f e ge

L24: Entry 2 of 4 File: USPT Oct 10, 2000

US-PAT-NO: 6131162
DOCUMENT-IDENTIFIER: US 6131162 A

TITLE: Digital data authentication method

DATE-ISSUED: October 10, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Yoshiura; Hiroshi	Kawasaki			JP
Takaragi; Kazuo	Ebina			JP
Sasaki; Ryoichi	Fujisawa			JP
Susaki; Seiichi	Yokohama			JP
Toyoshima; Hisashi	Hachioji			JP
Saito; Tsukasa	Tokyo			JP

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Hitachi Ltd.	Tokyo			JP	03

APPL-NO: 09/ 090419 [PALM]
DATE FILED: June 4, 1998

PARENT-CASE:
CROSS REFERENCE TO RELATED APPLICATIONS This application is related to application Ser. No. 09/385,638, filed Aug. 27, 1999, entitled "Method of Generating Authentication Enabled Electronic Data", by Y. Nagai et al; and application Ser. No. 09/371,526, filed Aug. 10, 1999, entitled "Method of Appending Information to Image and Method of Extracting Information from Image", by H. Yoshiura et al.

FOREIGN-APPL-PRIORITY-DATA:

COUNTRY	APPL-NO	APPL-DATE
JP	9-148061	June 5, 1997
JP	9-348860	December 18, 1997

INT-CL: [07] H04 L 9/32, H04 L 9/28, H04 L 9/30

US-CL-ISSUED: 713/176; 713/170, 713/181, 705/57, 380/28, 380/30
US-CL-CURRENT: 713/176; 380/28, 380/30, 705/57, 713/170, 713/181

FIELD-OF-SEARCH: 380/30, 380/28, 380/202, 380/279, 380/283, 705/51-58, 713/150, 713/155, 713/162, 713/168, 713/170, 713/176, 713/180, 713/181

PRIOR-ART-DISCLOSED:

h e b b g e e e f c e f e ge

U.S. PATENT DOCUMENTS

Search Selected | Search ALL | Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5530759	June 1996	Braudaway et al.	380/54
☐	5872848	February 1999	Romney et al.	380/25
☐	5892904	April 1999	Atkinson et al.	395/187.01
☐	5898779	April 1999	Squilla et al.	380/23
☐	5960081	September 1999	Vynne et al.	380/10

FOREIGN PATENT DOCUMENTS

FOREIGN-PAT-NO	PUBN-DATE	COUNTRY	US-CL
0855829	July 1989	EP	
0590884	April 1994	EP	
0705025	April 1996	EP	
0854633	July 1998	EP	
0859503	August 1998	EP	
53-148918	December 1978	JP	
6431198	February 1989	JP	

OTHER PUBLICATIONS

F. Rouaix, "A Web Navigator with Applets in Caml", 1996, Published by Elsevier Science B.V., Computer Networks and ISDN Systems 28, pp. 1365-1371.
S. Anderson, et al, "Sessioneer: Flexible Session Level Authentication with off the shelf servers and clients", 1995 Elsevier Science B.V., Computer Networks and ISDN Systems 27, pp. 1047-1053.
W. Bender, "Techniques for Data Hiding", IBM Systems Journal, vol. 35, No. 3 & 4, 1996, pp. 313-330.
N. Komatsu, et al, A Proposal on Digital Watermark in Document Image Communication and its Application to Realizing a Signature, Electronics and Communications in Japan 73(1990) May, No. 5, Part I, New York, US, pp. 22-33.
B. Schneier, Applied Cryptography 1996, John Wiley & Sons, US New York, pp. 39-41.
Sasaki, et al, Security Technology for Open Networks, Hitachi Review, JP, Hitachi, Ltd., Tokyo, vol. 46, No. 4, pp. 197-202.
M. Schneider et al, A Robust Content Based Digital Signature for Image Authentication, Proceedings of the International Conference on Image Processing, US, New York, IEEE, pp. 227-230.
W. Bender, Techniques for Data Hiding, IBM Systems Journal, vol. 35, No. 3 & 4, 1996, pp. 313-336.
Eiji Okamoto, Ango Riron Nyumon (Introduction to Cryptography), Kyoritsu Shuppan Co., Ltd., 1993, pp. 133-137.
Bruce Schneier, Applied Cryptography, 2.sup.nd Ed., John Wilsy & Sons, Inc., 1996, pp. 39-41.
Nikkei Electronics., No. 683, 1997, pp. 99-107.
Opendesign., Apr., 1996, pp. 4-22.
Opendesign., Apr. 1996, pp. 40-78.
Jyohoshori (Information Processing), Jyohoshori Gakkai (Information

Processing Society of Japan), vol. 38, No. 9, 1997, pp. 752-810.

ART-UNIT: 277

PRIMARY-EXAMINER: Swann; Tod R.

ASSISTANT-EXAMINER: Darrow; Justin T.

ATTY-AGENT-FIRM: Antonelli, Terry, Stout & Kraus, LLP

ABSTRACT:

This invention provides a method for identifying a purchaser who purchased content from which an illegal copy was produced. A provider system encrypts a content purchased by the purchaser using a public key of a purchaser system and sends the encrypted content to the purchaser system. The purchaser system creates a digital signature of the content with the use of a private key of its own and embeds the created digital signature into the received content. When an illegal copy is found, the provider system verifies the digital signature, embedded in the illegal copy as a digital watermark, to identify the purchaser who purchased the content from which the illegal copy was produced.

63 Claims, 29 Drawing figures

Previous Doc Next Doc Go to Doc#

h e b b g e e e f c e f e ge

L24: Entry 3 of 4 File: USPT Feb 8, 2000

US-PAT-NO: 6023509
DOCUMENT-IDENTIFIER: US 6023509 A

TITLE: Digital signature purpose encoding

DATE-ISSUED: February 8, 2000

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Herbert; Howard C.	Phoenix	AZ		
Davis; Derek L.	Phoenix	AZ		

ASSIGNEE-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY	TYPE CODE
Intel Corporation	Santa Clara	CA			02

APPL-NO: 08/ 720444 [PALM]
DATE FILED: September 30, 1996

INT-CL: [06] H04 L 9/00

US-CL-ISSUED: 380/25; 380/23, 380/29, 380/30, 380/49
US-CL-CURRENT: 705/76; 380/29, 380/30, 713/175, 713/180

FIELD-OF-SEARCH: 380/4, 380/9, 380/23, 380/24, 380/25, 380/29, 380/30, 380/46, 380/49, 380/50, 380/59

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	5005200	April 1991	Fischer	380/30
☐	5208858	May 1993	Vollert et al.	380/23 X
☐	5479509	December 1995	Ugon	380/23

ART-UNIT: 276

PRIMARY-EXAMINER: Gregory; Bernarr E.

h e b b g e e e f c e f e ge

ATTY-AGENT-FIRM: Blakely, Sokoloff, Taylor & Zafman

ABSTRACT:

A method and apparatus for encoding a purpose into a digital signature, where purpose and digital signature bound into an extended digital signature. The extended digital signature capability binds a purpose description identifying the purpose for the digital signature so that when affixed to a digital signature, the digital signature cannot be employed for improper purposes. A hash function is used to generate a hash value from the purpose description. The hash value is used in a digital signature function to bind the purpose to a digital signature. The extended digital signature can be verified for validity by comparing it to a hash value. In an electronic transaction, the extended digital signature can allow a purpose to be bound with the digital signature so that improper or unauthorized transactions are detected and disallowed.

14 Claims, 9 Drawing figures

Previous Doc Next Doc Go to Doc#

h e b b g e e e f c e f e ge

First Hit Fwd Refs Previous Doc Next Doc Go to Doc#
End of Result Set

Generate Collection Print

L24: Entry 4 of 4 File: USPT Sep 22, 1998

US-PAT-NO: 5812669
DOCUMENT-IDENTIFIER: US 5812669 A

TITLE: Method and system for providing secure EDI over an open network

DATE-ISSUED: September 22, 1998

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Jenkins; Lew	Pleasant Hill	CA	94523	
Pasetes, Jr.; Emmanuel K.	Danville	CA	94525	

APPL-NO: 08/ 503984 [PALM]
DATE FILED: July 19, 1995

INT-CL: [06] H04 L 9/00, H04 L 9/30, H04 L 9/32

US-CL-ISSUED: 380/25; 380/21, 380/23, 380/30, 380/49
US-CL-CURRENT: 713/161; 380/30, 705/75, 713/176, 713/181

FIELD-OF-SEARCH: 380/9, 380/21, 380/23, 380/25, 380/30, 380/44, 380/46, 380/49, 380/50

PRIOR-ART-DISCLOSED:

U.S. PATENT DOCUMENTS

Search Selected Search ALL Clear

	PAT-NO	ISSUE-DATE	PATENTEE-NAME	US-CL
☐	4200770	April 1980	Hellman et al.	
☐	4218582	August 1980	Hellman et al.	
☐	4267782	May 1981	Talbott	
☐	4405829	September 1983	Rivest et al.	
☐	4424414	January 1984	Hellman et al.	
☐	4471164	September 1984	Henry	
☐	4578531	March 1986	Everhart et al.	
☐	4625076	November 1986	Okamoto et al.	
☐	4723284	February 1988	Munck et al.	

h e b b g e e e f c e f e ge

☐	4823388	April 1989	Mizutani et al.
☐	4868877	September 1989	Fischer
☐	4876716	October 1989	Okamoto
☐	4885777	December 1989	Takaragi et al.
☐	4893338	January 1990	Pastor
☐	4987593	January 1991	Chaum
☐	4991210	February 1991	Chaum
☐	5001752	March 1991	Fischer
☐	5005200	April 1991	Fischer
☐	5018196	May 1991	Takaragi
☐	5022080	June 1991	Durst et al.
☐	5073934	December 1991	Matyas et al.
☐	5073935	December 1991	Pastor
☐	5136643	August 1992	Fischer
☐	5136646	August 1992	Haber et al.
☐	5142577	August 1992	Pastor
☐	5142578	August 1992	Matyas et al.
☐	5199074	March 1993	Thor
☐	5202977	April 1993	Pasetes, Jr. et al.
☐	5204961	April 1993	Barlow
☐	5208858	May 1993	Vollert et al.
☐	5214702	May 1993	Fischer
☐	5222140	June 1993	Beller et al.
☐	5224166	June 1993	Hartman, Jr.
☐	5226709	July 1993	Labrache
☐	5237611	August 1993	Rasmussen et al.
☐	5253294	October 1993	Maurer
☐	5261002	November 1993	Perlman et al.
☐	5268962	December 1993	Abadi et al.
☐	5297208	March 1994	Schlafly et al.
☐	5299263	March 1994	Beller et al.
☐	5303303	April 1994	White
☐	5311591	May 1994	Fischer
☐	5337360	August 1994	Fischer
☐	5339361	August 1994	Schwalm et al.
☐	5351293	September 1994	Michener et al.
☐	5351302	September 1994	Leighton et al.
	5367573	November 1994	Quimby

h e b b g e e e f c e f e ge

☐	5369702	November 1994	Shanton	
☐	5369705	November 1994	Bird et al.	
☐	5373558	December 1994	Chaum	
☐	5375169	December 1994	Scheidt et al.	
☐	5390247	February 1995	Fischer	380/25

ART-UNIT: 362

PRIMARY-EXAMINER: Gregory; Bernarr E.

ATTY-AGENT-FIRM: Bryan Cave LLP

ABSTRACT:

A method and system for selectively interconnecting a plurality of computers (112,114) over an open public network (120,102,122), such as the INTERNET, provides a private secure computer exchange of EDI interchange communications between a sender computer (112) and a recipient computer (114), each of which has an associated public key and an associated private key, such as in an RSA type cryptographic communication system (100). The associated EDI acknowledgement message, such as the AUTACK, is used to provide secure authentication and non-repudiation of both origin and receipt of the secure private EDI interchange communications transmitted over the open public network (120,102,122) with the AUTACK transmitted from the sender computer (112) being digitally signed with the sender's private key, and with the reply AUTACK transmitted from the recipient computer (114) being digitally signed with the recipient's private key. The respective digitally signed AUTACKs are decrypted after receipt by using the public key associated with the private key used to provide the digital signature. The transmitted AUTACK from the sender computer (112) includes an MD5 for the entire EDI interchange as well as an MD5 of the AUTACK, with the AUTACK, thus, being used to provide the digital signature. The reply AUTACK from the recipient computer (114) includes an MD5 of the reply AUTACK. The ability to conduct business over the network (120,102,122) is controlled by private trading partner agreement communications which provide key certification.

50 Claims, 43 Drawing figures

Previous Doc Next Doc Go to Doc#